PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-148697
(43)Date of publication of application : 29.05.2001

(51)Int.CI. H04L 9/32
G06F 12/14
G09C 1/00
H04L 9/10

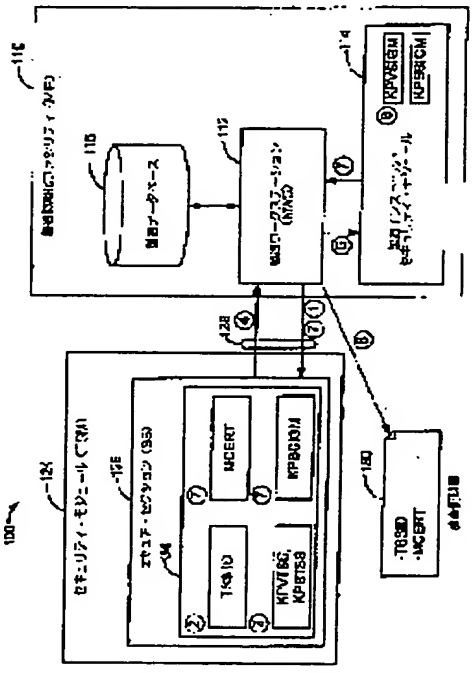
(21)Application number : 2000-262692
(22)Date of filing : 31.08.2000

(71)Applicant : COMPAQ COMPUTER CORP
(72)Inventor : HOPKINS DALE WEBSTER
MCKAY MICHAEL
LANGFORD SUSAN
HINES LARRY

(30)Priority
Priority number : 1999 389157 Priority date : 02.09.1999 Priority country : US

(54) METHOD FOR COMMUNICATING INFORMATION VIA CHANNEL HAVING LOW RELIABILITY

(57)Abstract:
PROBLEM TO BE SOLVED: To attain the communication security between the devices which are connected to a network.
SOLUTION: A secure section SS 126 of a security module TSM 124 included in a device stores the serial numbers SSID sent from a manufacturing initialization facility MIF 110 via a network into a storage 34 ((2)) and then generates and stores a public key pair ((3)). The public key pair includes a secret part KPVS and a public part KPBSS and transmits only the part KPBSS to the facility MIF 110 ((4)). A manufacturing install security module MISM 114 generates and stores a manufacturer certificate including the part KPBSS and a secret signature key KPVSIGM ((6)), and also the certificate is transmitted to the section SS 126 of the module TSM 124 and stored there together with a public signature key KPBSIGM of the facility MIF 110 ((7)). The facility MIF 110 also generates an inspection certificate 130. The internal secrecy is stored in every device and certificate and accordingly the devices can authenticate and safely communicate with each other even via a channel having low reliability without being previously programmed by means of the secrecy of an operator.



LEGAL STATUS
[Date of request for examination]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－148697
（P2001－148697A）
(43)公開日　平成13年５月29日(2001.5.29)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ　9/32		Ｇ０６Ｆ　12/14		３２０Ｂ
Ｇ０６Ｆ　12/14	３２０	Ｇ０９Ｃ　1/00		６６０Ｂ
Ｇ０９Ｃ　1/00	６６０	Ｈ０４Ｌ　9/00		６７５Ｂ
Ｈ０４Ｌ　9/10				６２１Ａ

審査請求　未請求　請求項の数11　ＯＬ　（全 16 頁）

(21)出願番号　特願2000－262692(P2000－262692)

(22)出願日　平成12年８月31日(2000.8.31)

(31)優先権主張番号　０９／３８９１５７

(32)優先日　平成11年９月２日(1999.9.2)

(33)優先権主張国　米国（ＵＳ）

(71)出願人　591030868
コンパック・コンピューター・コーポレーション
COMPAQ COMPUTER CORPORATION
アメリカ合衆国テキサス州77070，ヒューストン，スティト・ハイウェイ　249，20555

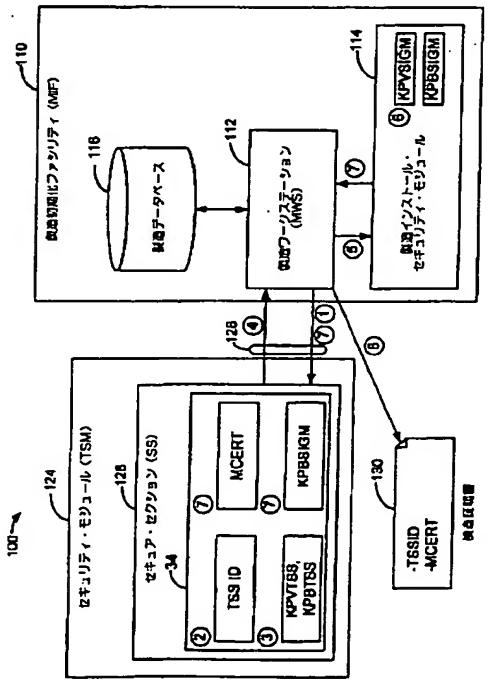
(72)発明者　デイル・ウェブスター・ホプキンス
アメリカ合衆国カリフォルニア州，サン・ホセ，ザンカー・ロード　2304

(74)代理人　100089705
弁理士　社本　一夫　（外５名）

最終頁に続く

(54)【発明の名称】　低信頼性のチャネルを介して情報を通信する方法

(57)【要約】
【課題】ネットワークに接続されるデバイス間の通信セキュリティを確立する。
【解決手段】デバイス内のＴＳＭ１２４のＳＳ１２６は、ＭＩＦ１１０からネットワークを介して送られた通し番号ＳＳＩＤを記憶装置３４に記憶し（②）、公開キー・ペアを生成し格納する（③）。該ペアは秘密部分ＫＰＶＳと公開部分ＫＰＢＳＳを備え、公開部分のみをＭＩＦに送信する（④）。ＭＩＳＭ１１４は、該公開部分及び秘密署名キーＫＰＶＳＩＧＭを有する製造業者証明書を生成し、記憶する（⑥）とともに、ＴＳＭ１２４のＳＳ１２６に送信され、ＭＩＦの公開署名キーＫＰＢＳＩＧＭとともに記憶される（⑦）。ＭＩＦ１１０は、検査証明書１３０も生成する。内部機密が各デバイス及び証明書内に保持されるので、デバイスは、オペレータの機密を用いて予めプログラムされる必要無く、低信頼性のチャネルを介してでも、相互認証して安全に通信することができる。



【特許請求の範囲】

【請求項１】　オペレータに作用する他のデバイスと通信するための、該オペレータによって使用されるデバイスを製造する方法であって、製造業者は該製造業者及びその認可されたエージェント以外の他人にとって通常は入手不可能である製造業者キーを有し、通信が盗聴又はメッセージ変更から安全であることが保証されていない信頼性の低いチャネルによって行われる、デバイス製造方法において、

オペレータに関する機密を含む必要がなくかつ変形不可能境界内に含まれる回路としてのセキュア・セクションを含むように、デバイスを製造するステップと、

製造されたデバイスに特定のデバイス識別子を用いてデバイスを初期化する初期化ステップと、

セキュア・セクションをトリガして、内部機密を生成するステップと、

セキュア・セクション内に、内部機密の非可逆性の暗号化変換を作成するステップと、

デバイスから、非可逆性の暗号化変換を内部機密の公開部分として出力するステップと、

製造業者キーを使用して、該公開部分及びデバイス識別子のデジタル署名を生成するステップとを含むことを特徴とする方法。

【請求項２】　請求項１記載の方法において、各デバイスは、特定のオペレータ又は該デバイスが接続されるネットワークに限定されていない、一般的なデバイスとして製造されていることを特徴とする方法。

【請求項３】　請求項１記載の方法において、該方法は更に、デバイスが適切に製造されたことを認証するためのステップを含むことを特徴とする方法。

【請求項４】　請求項１記載の方法において、非可逆性の暗号化変換を作成するステップは公開キーのペアを生成するステップを含み、該公開キーのペアの公開キー部分が内部機密の公開部分となることを特徴とする方法。

【請求項５】　公開部分と製造業者キーを用いる一意のデバイス識別子とのデジタル署名が存在する内部機密を有するデバイスを使用して、信頼性の無いチャネル環境において、デバイスとキー・サーバとの間に安全チャネルをセットアップする方法において、

デバイスに対してキー・サーバを認証する第１の認証ステップと、

内部機密を知っているデバイスのみが生成することができる応答を提供するようデバイスに要求することにより、キー・サーバに対して該デバイスを認証する第２の認証ステップと、

第１及び第２の認証ステップにおいてキー・サーバ及びデバイスによって提供された情報を用いて、キー・サーバ及びデバイスによって共有される共有機密を作成するステップと、

チャネルを介しての安全な通信のために、共有機密を使用するステップとを含むことを特徴とする方法。

【請求項６】　請求項５記載の方法において、共有機密を使用するステップは、キー・サーバとデバイスとの間でデータを転送すること、キー・サーバとデバイスとの間でキーを転送すること、デバイスにおいてコンフィギュレーション値をセットすること、及び、デバイスからコンフィギュレーション値を読出すことの少なくとも１つを含むことを特徴とする方法。

【請求項７】　ターゲット・デバイスとキー・サーバとの間で信頼性の低いチャネルを介してキー・サーバからターゲット・デバイスにキーをロードする方法であって、該ターゲット・デバイスの初期コンテンツが、信頼性の無いエンティティによって決定可能であると推定される、キー・ロード方法において、

ターゲット・デバイスの安全な回路内で、予め値を決定することができない少なくとも１つの変数の関数であるセッション・キーを生成するステップと、

信頼性の無いチャネル上に保護されたチャネルを構成する際に、セッション・キーを使用するステップと、

護されたチャネルを用いて、キー・サーバからターゲット・デバイスに少なくとも１つのキーをロードするステップとを含むことを特徴とする方法。

【請求項８】　請求項７記載の方法において、ターゲット・デバイスは、安全なネットワークに付加されるべき新たに製造された端末であり、機密を有していないと推定されることを特徴とする方法。

【請求項９】　信頼性の無いチャネルを介してキー・サーバからターゲット・デバイスに安全にキーをロードするシステムにおいて、

ターゲット・デバイス内に設けられ、（ａ）乱数発生器と、（ｂ）指数演算器と、（ｃ）乱数発生器と指数演算器の出力に基づいて、機密セッション・キーがロジック装置に関する知識及びその製造された状態とからは容易に生成することができないように、機密セッション・キーを生成するロジック装置とを備えたセキュア・チップと、

キー・サーバ内に設けられ、機密セッション・キーで符号化された該ターゲット・デバイスによって受信されるメッセージを解読し、該解読されたメッセージを用いて信頼性の無いチャネルを介してセキュア・チャネルを起動するキー・サーバ・ロジック装置とを具備することを特徴とするシステム。

【請求項１０】　信頼性の低いチャネルを介して初期化キーでセキュリティ・デバイスを初期化する方法において、

機密であることが知られていないハードウェア構成のセキュリティ・デバイスの保護された部分内に機密を生成するステップと、

生成された機密を用いて、セキュリティ・デバイスと外部ノードとの間で安全に通信するステップとを含むこと

を特徴とする方法。

【請求項１１】　請求項１０記載の方法において、外部ノードは、キー・サーバに関連付けられたノードであり、該方法はさらに、生成された機密キーを用いて確立された安全な通信チャネルを介して、キー・サーバからセキュリティ・デバイスに少なくとも１つのキーをロードするステップを含むことを特徴とする方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号化システムに関し、特に、安全な（ｓｅｃｕｒｅ）初期化を必要とする暗号化システムに関する。

【０００２】

【従来の技術】通信及びデータ記憶デバイスを好ましくないアクセス及び改変（改竄）から保護するために、暗号化が使用されている。安全な通信には、いくつかの特徴がある。安全な通信の１つの特徴は、保護されたメッセージが、メッセージ送信側とメッセージ受信側以外のエンティティによっては読取ることができない、ということである。安全な通信の他の特徴は、受信側にメッセージが変更されたことを検出されないように、アタッカが送信側から受信側に伝送中のメッセージを変更することができない、ということである。メッセージをその変更が検出可能な方法で変更したとしても、大した問題ではない。すなわち、受信側が、変更されたメッセージを明らかな偽造又は通信エラーであるものとして、単純に破棄することができるためである。

【０００３】当然のことながら、実現可能な安全な通信により、十分な時間、労力及びコンピュータの能力があれば、メッセージを読出し可能又は変更可能にすることができる。このような能力があっても、アタッカが、メッセージに対する解読キーを有するか、又は、メッセージを「クラッキング」してその内容を読出すか又は変更されたメッセージを作成して、時間又は計算能力をその許容閾値を超えて消費するかしなければ、メッセージを読出すか又は変更することができない場合、メッセージは、読出し不可能か又は変更不可能であると推定される。一般に、安全な通信システムは、時間の閾値が、メッセージが機密であり続ける必要がある時間の長さより長いように設計されており、計算能力の閾値は、アタッカがメッセージをクラッキングすることによって取得する利益に見合ったコストであらゆる予測されたアタッカに入手可能な計算能力より、大幅に大きい。

【０００４】より一般的に述べると、暗号化システムは、該暗号化システムによって保護される通信又はデータ記憶システムの使用を制限するために採用される１つ又は複数の機密を保持するシステムである。なお、本明細書において、「通信システム」とは、伝統的に通信システムとして考えられなかったシステムを含んでおり、あるソース（すなわち送信元）からあるデスティネーション（すなわち送信先）にデータを通信する場合、又は、安全な方法でデータをデータ記憶デバイス間で転送する（すなわち、データの書き手側からデータの読み手側への「通信」を安全にする）場合の、あらゆるシステムを意味している。

【０００５】１つ又は複数のメッセージを機密保護する際に、一般的な暗号化システムは、メッセージを機密のままにし、またメッセージの認証、完全性、及び非支払拒否性を確実にするために、使用される。当然のことながら、暗号化システムによっては、それら機能をすべて行うとは限らない。例えば、あるものは、文書を認証するためのシステムをセットアップするが、該認証された文書は、すべての視聴者が見れるようにオープンにされる。認証により、受信側は、メッセージの送信側と称している送信側が実際の送信側であるか否かを検査することができ、完全性により、受信側は、受信したメッセージがまさに送信されたメッセージであるか否かを検査することができ、非支払拒否性により、受信側は、メッセージが送信側によって実際に送信されたということを、送信側及びその他に証明することができる。

【０００６】通信システムの設計によっては、センシティブな暗号化オペレーションを厳密に制御することができるように、暗号システム・モジュールにおいて、暗号化機能が他の機能から分離されている。一般的な暗号システム・モジュールは、メッセージを暗号化し、解読し、照合するために使用するための機密を保持する。これら機密は、しばしば「キー」と呼ばれる。キーは、記憶されたデータを保護するか、通信チャネルを保護するか、又は、他の同様のタスクを保護するために使用することができる。データ又は通信チャネルを保護することにより、そのデータ又はチャネルの使用を、アクセスを保護するために使用されるキーを知っている人々又はエンティティのみに限定することができる。

【０００７】通信チャネルを保護する際のキーの使用法には、いくつもの方法がある。１つの使用法は、メッセージの暗号化／解読に関係するものである。この使用法において、ソースからデスティネーションに通信するために使用されるチャネルは、必ずしも安全ではないと考えられる。安全でないチャネルは、アタッカがソースからデスティネーションに移動するトラフィックを盗聴する、「盗聴（ｅａｖｅｓｄｒｏｐｐｉｎｇ）」アタックに晒されやすい。また、安全でないチャネルは、アタッカがトラフィック内を盗聴する能力を有するだけでなく、それがソースからデスティネーションに進む際にメッセージを変更することもできる、「マン・イン・ザ・ミドル（ｍａｎ－ｉｎ－ｔｈｅ－ｍｉｄｄｌｅ）」アタックにも晒され易い。信頼性の無いチャネルは、実際には安全である場合も安全でない場合も有り得るが、安全でないと推定されるチャネルである。信頼性の無いチャネルに対して設計されているセキュリティ・システム

は、チャネルがある観点で安全ではないと推定するが、該システムは、システム設計によって付加されたセキュリティ基準無しに安全となるチャネルを介する場合と同じ方法で動作することになる。

【０００８】ソースからデスティネーションへのトラフィックを暗号化することにより、これらのアタックを受けてしまうことを、大幅に困難なものにすることができる。暗号化により、プレインテキスト（平文）・メッセージ（すなわち、メッセージを所有していれば誰でも読出し可能なメッセージ）が、キーを用いて、暗号文メッセージに変換される。そして、このキーを知らなければ、暗号文がプレインテキスト・メッセージに容易に戻すことができない。暗号化は、プレインテキスト・メッセージとキーとをプロセス入力とする暗号化プロセスを用いて行われる。好ましくは、メッセージのセキュリティは、暗号化プロセスの詳細を知らないアタッカによるものではない。暗号化プロセスは全く周知であって、セキュリティがアタッカに知られていないキーによってのみ提供される、という暗号化システムが、より好適である。

【０００９】安全な通信の上述した各々の有用性は、ポイント・オブ・セール（ＰＯＳ）端末ネットワークに関して説明することができる。ＰＯＳ端末ネットワークにおけるＰＯＳ端末は、商店と顧客との間の販売を容易にするために使用される。このＰＯＳ端末ネットワークでは、顧客は、販売をカバーするべく、その顧客の銀行預金口座から商店の銀行預金口座に資金を振替るよう、顧客の銀行に許可する。取引は、商店のＰＯＳ端末と他のネットワーク・デバイスとの間で１つ又は複数のメッセージを通信することによって行われる。ＰＯＳ端末ネットワークの１つの目的は、通信を保護することであるため、盗聴者又は窃盗犯（一般に、多くの暗号化テキストにおいて「アタッカ」と呼ばれる）は、メッセージ・キーを知らなければ、メッセージ・トラフィックを読み出すことも不可能であり、また、検出されることなくデータを変更することもできない。

【００１０】明らかなように、販売取引に関わる当事者は、メッセージ・トラフィックが安全な通信の上述した態様を有していることを望む。顧客は、自身の口座番号がアタッカによって読出し不可能であるように、通信が機密であることが確実であるよう望む。銀行は、資金が顧客によって正式に認められた時にのみ引出されるように、通信が信頼できることが確実であることを望む。アタッカが商店の口座番号をアタッカの口座番号に置換えるようにメッセージを編集することができないように、メッセージの完全性が保証されている必要がある。また、顧客が買って帰った商品に対し銀行が商店に支払いを行ったが、その顧客が取引を拒否し自身の口座から取引を取り消したいという場合が生じないようにするため、非支払拒否は、顧客の銀行にとって重要である。

【００１１】安全な通信のこれらの面は、銀行及び顧客がこれらの間の通信を保護するステップをとる場合に、確実にすることができる。銀行の方が顧客よりもインフラストラクチャに関わる可能性が高いため、セキュリティにおける顧客の関わりは、一般に、パスワード（「キー」）の選択とパスワードの機密を保持することとに限られる。顧客のタスクがキーを記憶するという簡単なことであるが、銀行のタスクはより複雑である。これは、アタッカが通信に介入して通信を安全でないものにする機会が多くあるためである。リスクもまた、顧客よりも銀行の方がずっと大きい。顧客のセキュリティが破られ、アタッカが顧客のパスワードを取得した場合、アタッカの取り分は通常、１人の顧客の銀行預金口座で入手可能な資金に制限される。顧客が処理中に権限の無いアクティビティに気が付いた場合、その取り分は更に制限される。しかしながら、銀行のセキュリティが危険に晒されている場合、アタッカの取り分は制限されず、かつ人目を引かない。このため、銀行は、安全システムを有することに非常に関心を持っている。

【００１２】公開キー暗号化が使用される場合、一対のキーが生成され、そのうちの一方が秘密キーであり、他方が公開キーである。いずれの場合も、安全な端末は秘密キーを有している。アタッカは、それら秘密キーを取得することができる場合、安全な端末間を行き来するメッセージ・トラフィック上で盗聴することができ、そのトラフィックをインタセプトすることさえできる場合がある。また、場合によっては、秘密キーを知っているアタッカが、安全な端末を宛先とするメッセージを変更し、安全な端末によって送信されているメッセージを変更するために十分な知識を有している場合がある。それによって、アタッカは、検出されることなく、以降のメッセージ・トラフィックを変更し続けることができる。かかる危険性は、アタッカが「キー変更」コマンドと新たな秘密キーとを含むメッセージをインタセプトすると、秘密キーが変更された後でも継続する。

【００１３】アクセスが続けられることにより、危険に晒された端末は危険に晒された端末であり続ける。逆に、保護された端末は、通常、適切に設計されている場合、安全な端末であり続けることができる。安全なシステムは、一旦危険に晒されると、安全なシステムと見なすことができない。従って、安全なシステムは、システムの最初のインストールを含む各インプリメンテーション段階において、安全であることが必要である。最初のインストールでの困難の１つは、端末が秘密キーの初期セットで開始する必要がある、ということである。秘密キーの初期セットは、新たなキーとキーを変更するという命令とを含む保護されたコマンド・メッセージを端末に送信することにより、遠隔制御で変更することができる。「キー変更」メッセージが送信される前に端末が危険に晒された場合、アタッカがメッセージを読出しその

キーのコピーを更新することができるため、それによって危険性が継続する。暗号化システムの上記脆弱性を鑑みると、暗号化デバイスの初期化プロセスは、暗号化デバイスが安全であるように、注意深く設計されなければならない。

【００１４】

【発明が解決しようとする課題】デバイス初期化の１つの解決法は、製造中にキーの初期セットをインストールするというものである。この解決法の欠点は、製造業者が各デバイスの初期キーを追跡し続けなければならないということ、及び、端末の購入者が、その情報を安全にしておくために、製造業者に頼らなければならないということである。初期キーが明白にロードされている場合、プロセスを監視している人は誰でもそのキーを獲得することができ、デバイスのセキュリティを脅かすことができる。あるいは、製造業者は、デバイスがすべて共通の初期キーを有するようにデバイスを製造してもよい。共通の初期キーによって、盗聴者からは安全に最初の一意のキーをロードすることは可能であるが、多くのデバイスに共通のキーのセキュリティは、通常、信用できないものである。

【００１５】デバイス初期化の他の方法は、「信用されたエージェント（ｔｒｕｓｔｅｄａｇｅｎｔ）」方法である。この方法により、暗号化システムは、キー無しに製造され、安全なチャネルによりキーを暗号化システムに入力することによって、暗号化システムの所有者の信用されたエージェントによって初期化される。暗号化システムが安全でないコネクションによって接続されたリモート・ネットワーク（グローバル・インタネット等）上に配置されている場合、信用されたエージェントは、初期化キーを入力するために暗号化システムのロケーションに移動しなければならない。一般に、エージェントの従業員すべてを必ずしも完全に信用できるものでないため、初期化キーは、エージェントの２人の信用された従業員間に分割される。彼らは、初期化キーのそれぞれの部分を入力するために、暗号化システムのロケーションに各々移動する。当然のことながら、これは費用がかかりかつ時間がかかる。更に、キー入力のためのキーボード等の専用ハードウェアが使用される場合、その分のコストがデバイスに付加され、キーのロードの自動化が妨げられる。

【００１６】信用されたエージェントによる方法は、目下、初期キーを新たなＡＴＭ（自動預金支払機）及びＰＯＳ端末（本明細書では包括的に「端末」と言う）にロードするために使用されている。ＤＥＳキー部分の二重管理を提供する少なくとも２人のセキュリティ人員は、キー・ロード・デバイスから端末への実際のキーのロードを監視する。一般的なネットワークがかかる端末を何万も有している場合が多いため、このキー・ロード・プロセスは、特にデビットＰＯＳ端末の場合に、非常に負担となる。

【００１７】リモート・ロケーションへの移動を避けるために、キー貯蔵所（ｄｅｐｏｔ）を使用することができる。キー貯蔵所は、すべての暗号化システムが製造後に導かれる安全なロケーションである。このキー貯蔵所において、初期化キーが安全なチャネルを介して暗号化システムにロードされ、その後、暗号化システムは使用される場所に移送される。この方法は、実際の取引では物理的なキー貯蔵所の保持を継続しなければならず、いくつかの余分の移送ステップが必要であるため、コストがいくらか低減するにも関わらず、実質的に別の費用がかかる。

【００１８】

【課題を解決するための手段】本発明の１つの実施の形態による暗号化システムにおいて、内部機密を生成するセキュア・セクションを有するデバイスが製造される。内部機密の非可逆性暗号化変換が行われ、非可逆性暗号化変換及びデバイスの一意の識別子を含む証明書（ｃｅｒｔｉｆｉｃａｔｅ）に対し、製造業者のキーを用いて署名がなされる。デバイス及び証明書は、ネットワーク・オペレータに提供される。そのオペレータの制御の下、初期化プロセスが実行されることにより、２つのデバイス間の安全な通信のために、オペレータの制御の下で、２つのデバイス間に安全なチャネルがセットアップされる。各デバイス内に保持される内部機密及び証明書により、それらデバイスは互いを認証することができ、それらデバイスがオペレータの機密によって予めプログラミングされている必要なく、安全でないチャネルを介する場合であっても、安全に通信することができる。それらデバイスは、互いを認証することができ、安全でないチャネル全体に亘って共有機密を作成することができる。

【００１９】

【発明の実施の形態】本発明は、この開示を読めば明らかとなるように、多くのアプリケーションを有している。本発明によるセキュリティ・モジュールの実施の形態の説明においては、可能な変形例を例示的に説明している。更に、この説明において、セキュリティ・モジュールの特定のアプリケーションが、一例として繰返し用いられている。当業者には、他の適用法及び変形例が明らかとなろう。そのため、本発明は、実施例のように狭く解釈されるべきではなく、添付の特許請求の範囲に従って解釈されるべきである。

【００２０】本システムの説明において繰返し使用されている１つの特定のアプリケーションは、銀行により、その銀行とその顧客との間のメッセージを制御するためにセキュリティ・モジュールを使用することである。銀行は、その資金及び顧客を保護するものであり、資金振替メッセージ及び他の通信が内密で確実であり完全であることを保証すべきである。預金者の資金の強固な保管

者であるために、銀行は、製造業者、銀行の顧客、又は銀行の従業員を完全に信用している訳ではなく、これらが、メッセージ・トラフィック上で盗聴するか、あるいは、内密のメッセージを読出すようトラフィックを変更するため干渉するか、又はインタセプトする者がまったく権限の無い預金口座から資金が転送されるようにするよう、改竄することが全く無いとは考えていない。

【００２１】図１は、銀行又は他のセキュリティに関心があるエンティティによって使用することができるコンピュータ・システム１０の一例を示している。システム１０において、ネットワーク１２上に種々のデバイスが相互接続されている。本明細書において、「製造業者」は、デバイスを作製するエンティティか、又はそのデバイスの製造業者と利害関係を持って提携しているエージェント又は他のエンティティを説明するために使用される。「オペレータ」は、デバイス又はそのエージェントを使用することから利益を得るエンティティ、例えば、オペレータがそのオペレータのデータを送信するためにネットワーク１２上にセットアップした、安全なネットワークに、インストールするためにデバイスを購入した購入者を説明するために使用される。本発明において、製造業者とオペレータとは別個のエンティティである必要はまったく無いが、セキュリティの目的で、オペレータの関心は、オペレータが必ずしも製造業者を信用していないということであると想定する。

【００２２】ネットワーク１２は、信頼性の無いネットワークであるが、本発明は、信頼性の無いネットワークの使用に限定されるものではない。使用可能なネットワークの一例は、ネットワークのうち、一般に「インターネット」として知られるグローバル・インターネットワークである。インターネットは、ほとんど設計により、パケットのルーティングが概して制御されておらず、パケットが、送信側にも受信側にも未知でありかつ制御されない多くの異なるコンピュータ・システムを通してルーティングすることができるため、必ずしも安全ではない。上記ルーティングにより、ルーティング・コンポーネントにアクセスするアタッカは、データを盗聴することも変更することも可能である。

【００２３】ネットワーク１２に接続されている図１に示すデバイスとして、端末１４及び安全キー及びデータマネージャ（ＳＫＤＭ）１６が示されており、それらの動作は後に詳述する。説明の目的のために、権限の無いすなわち非認可端末１４’及び非認可ＳＫＤＭ１６’がネットワーク１２に接続されている。かかる非認可デバイスはネットワーク１２に容易に接続可能であるが、後述するように、認可された端末１４及びＳＫＤＭ１６のアーキテクチャ及びコンポーネントにより、非認可デバイス１４’、１６’は、認可されたデバイスと適切に相互動作が不可能である。

【００２４】図２は、端末１４の１つの実施の形態をより詳細に示している。図２は端末１４のブロック図であるが、ＳＫＤＭ１６を同様に構成することも可能である。端末１４は、入力／出力（Ｉ／Ｏ）セクション２０と、端末専用ロジック・ブロック２２と、セキュリティ・モジュール（ＳＭ）２４とを備えている。一般的なセットアップでは、端末のオペレータは、端末を製造業者から購入し、オペレータが、自分に特有の目的で使用するために、ネットワーク１２上にそれらをインストールする。

【００２５】セキュリティ・モジュール２４は、セキュア・セクション（ＳＳ）２６と非セキュア（非保護）・セクション２８とを備えている。適切に設計されたセキュア・セクションは、改変不可能すなわち改竄不可能（ｔａｍｐｅｒ－ｒｅｓｉｓｔａｎｔ）境界等、適切に設計されたセキュア・セクションに共通するいくつかの特性を有している。改変不可能境界により、アタッカが、配線の切断又はメモリの消去等の、少なくとも明確な破壊の証拠を残すことなく、セキュア・セクションの内部要素に到達することは困難となっている。他の特性は、セキュア・セクションが、侵入が完了してアタッカが機密へのアクセスを取得する前に、侵入が進行中であり機密を消去又は破壊している時にそれを検出する改変検出機構を有していることである。更に、適切に設計されたセキュア・セクションは、セキュア・セクションが改変不可能境界内で保護されたいかなる機密をも解放するような信号、データ入力、又はコマンドが存在しないため、論理的に安全である。

【００２６】非セキュア・セクション２８は、ＳＳ２６と端末１４の残りの部分との間のＩ／Ｏインタフェース等、セキュリティ・モジュール２４の動作をサポートするロジック及びデータを含み、該ロジック及びデータは、が安全が維持される必要のないものである。ＳＳ２６には、機密データ要素も非機密データ要素も格納することができるが、メモリが読出されないように保護する必要がある別のロジックが機密データ要素のみを保護する必要があるので、それらを別々に保持していることが好ましい。

【００２７】図３は、ＳＳ２６のより詳細なブロック図である。ＳＳ２６は、セクションＩ／Ｏ３０と、プロセス・ロジック３２（ゲート又はマイクロプロセッサ等）と、記憶装置３４と、乱数発生器（ＲＮＧ）３６と、指数演算器３８とを有している。記憶装置３４に記憶されるデータの詳細は、ＳＳ２６によって実行される種々のプロセスに関連して後述する。暗号化システムの設計において周知であるように、セキュリティ・オペレーションによっては、乱数と指数値とによるものがあるため、アタッカは、乱数発生器（ＲＮＧ）３６によって発生する乱数と指数演算器３８が実行する指数法とを制御又は観測することにより、システムのセキュリティを破ることができる。従って、乱数発生器（ＲＮＧ）３６及び指

数演算器３８は、好ましくはＳＳ２６の改変不可能境界内で保護されている。

【００２８】ここで、端末を動作させるプロセスを説明する。端末専用ロジック・ブロック２２の初期化は、端末の特定の使用法によって決まるものであり、それは、ここでの説明の範囲外であるため、焦点をセキュア・セクション２６の初期化に置く。ＳＳ２６の初期化を２つの部分で説明する。第１の部分は、ＳＳ２６の製造業者によって行われる動作を詳述し、第２の部分は、ＳＳ２６のオペレータによるか又はオペレータのために行われる動作を詳述する。図４にはＳＳ製造プロセスが示されている。示されている製造環境１００において、製造初期化ファシリティ（ＭＩＦ）１１０は、製造ワークステーション（MWS）１１２を備えている。ＭＳＷ１１２は、ＭＩＦ１１０内で安全な製造インストール・セキュリティ・モジュール（ＭＩＳＭ）１１４に結合されている。また、ＭＩＦ１１０は、ＭＩＦ１１０によって初期化されるセキュリティ・モジュールに関するデータを含む製造データベース１１６を有している。

【００２９】ターゲットであるＳＳ１２６を有するターゲットＳＭ１２４が、リンク１２０を介してＭＩＦ１１０に連結されている。以下に述べるプロセスにおいて、ターゲットＳＭ１２４は、初期化中のＳＭである。リンク１２０は、データ改変からのみ安全である必要がある。すなわち、ターゲットＳＳ１２６からMWS１１２に送信されるデータは、変更されずにMWS１１２によって受信され、MWS１１２からターゲットＳＳ１２６に送信されるデータは、ターゲットＳＳ１２６によって受信される。また、リンク１２０は、盗聴から安全であるようにすることが可能であるが、それは、ターゲットＳＳ１２６の初期化の全体的な完全性を維持するためには必要ではない。

【００３０】初期化プロセスに先立って、ターゲットＳＳ１２６を包括的なもの（ｇｅｎｅｒｉｃ）、すなわち、個々のターゲットＳＳ１２６は同一であるとすることができる。ターゲットＳＳ１２６は、ＭＩＦ１１０によって初期化プロセスが実行されることによって、包括的でなくなる。１つのかかる初期化プロセスの詳細は、図４において順序付けられたステップを示す○で囲まれた数字によって示されている。対応する数字は、下記の本文において、対応するステップの近傍に挿入されている。

【００３１】最初に、ＭＩＦは、ターゲットＳＳに対して通し番号ＳＳＩＤを生成し、ＳＳＩＤをターゲットＳＳに渡す（ステップ１）。ターゲットＳＳは、記憶装置３４にＳＳＩＤを記憶し（ステップ２）、公開キー・ペアＫＳＳを生成して（ステップ３）記憶装置３４に公開キー・ペアを格納する。ＫＳＳは、秘密部分ＫＰＶＳＳと公開部分ＫＰＢＳＳとを有している。ＫＳＳの生成は、ＳＳＩＤの受信、ＭＩＦからのコマンドの受信又は他の適切なトリガによってトリガすることができる。ターゲットＳＳは、ＫＳＳを生成すると、公開部分（ＫＰＢＳＳ）をMWSに送信する（ステップ４）。ターゲットＳＳがインストールされるシステムの全体のセキュリティの一部として、秘密部分ＫＰＶＳＳは、ターゲットＳＳ内に残り、ターゲットＳＳの外側と通信する必要が無くなる。

【００３２】ＭＳＷはＫＰＢＳＳ及びＳＳＩＤをＭＩＳＭに提供し、ＭＩＳＭは製造業者証明書ＭＣｅｒｔを生成する。製造業者証明書は、ＫＰＢＳＳを含んでおり、ＭＩＦ秘密署名キーＫＰＶＳＩＧＭによって署名され、ＭＩＳＭ内に保持される（ステップ６）。ＭＩＳＭは、ＭＩＦによって任意のＳＳが初期化される前に、ＭＩＦ署名キー・ペア（ＫＰＶＳＩＧＭ，ＫＰＢＳＩＧＭ）によって初期化される。また、製造業者証明書は、ＳＳＩＤ、証明書バージョン番号、デバイス許可（ターゲットＳＳに対する）及びアルゴリズム・パラメータ（ターゲットＳＳによって使用される）を含むことができ、それらの使用法は以下に説明されている。製造業者証明書は、ＭＩＳＭからターゲットＳＳに渡され、ターゲットＳＳ内において、ＭＩＦの公開署名キーＫＰＢＳＩＧＭと共に記憶される（ステップ７）。ＫＰＢＳＩＧＭもまた、ターゲットＳＳ内に記憶されるものである。また、ＭＩＦは、ＳＳＩＤ及びＭＣｅｒｔのコピーを含む検査証明書１３０を生成する（ステップ８）。

【００３３】この時点で、ターゲットＳＳは、正式に製造されたデバイスとなる。それは、特定の識別子（ＳＳＩＤ）を有しているため、非包括的ではあるが、一般にターゲットＳＳを使用する最終的なオペレータに特有なものではない。しかしながら、ターゲットＳＳは、各オペレータに対して異なるＭＩＦ署名キー・ペア（ＫＰＶＳＩＧＭ，ＫＰＢＳＩＧＭ）を使用することにより、オペレータに特有なものとすることができる。いずれにしても、ターゲットＳＳは、好ましくはこの時点でいかなるオペレータ機密をも含んでいない。以下に、オペレータがセットアップしたネットワークに対して、デバイスを特有なものにコンフィギュレーションするための初期化プロセスを説明する。

【００３４】ターゲットＳＳがオペレータに与えられる時、そのオペレータには、ターゲットＳＳに属する検査証明書１３０が与えられる。検査証明書は、それ自体保護された証明書である必要はないが、好ましくは、オペレータに対して個別に密かに与えられる。検査証明書により、オペレータは、密かに引き渡されたターゲットＳＳが、所定の一意的な識別子（ＳＳＩＤ）を有しておりかつ製造業者によって適切に初期化されている、ということを確認することができる。そして、オペレータは、ターゲットＳＳをＳＭ２４内にＳＳとしてインストールすることができる。あるいは、製造業者は、ＳＭ２４内にすでにインストールされているＳＳを提供するか、又

は、端末１４又はＳＫＤＭ１６にすでにインストールされているＳＳをＳＭ２４に提供することも可能である。

【００３５】オペレータは、ターゲットＳＳを取得すると、該ターゲットＳＳをネットワーク１２（安全でない可能性が高い）に接続する。一般に、オペレータは、ネットワーク１２上で１つ又は複数のＳＫＤＭを実行し、ＳＳによってとられる第１の動作は、キー・ロード・キー及びキー変更キー等の、オペレータ機密をＳＫＤＭからＳＳにローディングすることである。オペレータのセキュリティに対する関心の１つは、ＳＫＤＭが権限のない端末すなわち非認可端末１４’にキーをローディングしないこと、及び、ＳＳが非認可ＳＫＤＭ１６’からコマンド及びキーを受入れないということである。従って、ＳＳ及びＳＫＤＭは、オペレータ機密を脅かすために使用することができるいかなるオペレータ機密又はデータが転送される前に、互いを認証しなければならない。

【００３６】オペレータ初期化プロセス（初期化プロセスの第２の部分）において、ＳＳ及びＳＫＤＭ（又は、更に言えば２つのＳＳ）は、信頼性の無いチャネルによって接続される。なお、このプロセスは、安全でないネットワークに接続されたデバイスによって行うことができ、その場合、データは観測も変更も可能な状態である。このプロセスは、デバイスにおいてオペレータ機密のインストールを先に行うことなく実行することができる。

【００３７】オペレータによって操作される２つのデバイス間で使用可能な特定の相互認証プロセスの一例が、図５のフローチャートに示されている。図５に示したプロセスの変形例は、この説明から当業者には明らかとなるであろう。図５のフローチャートのステップは、ステップＳ１から始まる番号が付されており、それら番号は、括弧を用いて、以下の本文に挿入されている。これらステップは、番号が付された順序で実行されるが、当業者にとっては、この説明から、番号の大きい１つのステップに対しそれより番号の小さいステップがその番号の大きいステップの前に行われる必要がない場合、ステップの順序を変更することができることは、明らかであろう。

【００３８】図５に示すプロセスは、２つのデバイス、すなわちデバイスＡ及びデバイスＢを相互に認証し、その結果、デバイスＡ及びデバイスＢのみに既知の共有機密を生成する。当然のことながら、アタッカの計算能力又は時間が十分ある場合、共有機密はアタッカによって取得が可能であるため、システムは、計算能力又は時間が労力に見合わずにアタックを行うには高過ぎるように設計されていなければならない。後述するプロセスの１つの利点は、共有機密の生成が相互認証プロセスと絡み合っている、ということである。プロセスの他の利点は、認証センタ及び２つのデバイス間の認証チェーンを必要とすることなく、相互認証プロセスを行うことができる、ということである。デバイスＡは、端末１４でもＳＫＤＭ１６であってもよい（より正確には、それらデバイスのうちの１つのＳＭ２４）。また、デバイスＢは、端末１４であってもＳＫＤＭ１６であってもよい。例えば、デバイスＡ、Ｂは、端末とＳＫＤＭとであってもよく、又は両デバイスとも端末であってもよい。

【００３９】プロセスは、デバイスＡが認証のためにキー折衝キー（ＫＮＫ）のペア（ＫＰＶＡ１，ＫＰＢＡ１）を生成することから開始する（ステップＳ１）。上述した製造プロセスに続いて、デバイスＡは、一意的すなわちデバイスＡに特定の識別子（図５においてID_Aとラベル付けされている）、内部機密ＫＰＶＡ及びデバイスＡの製造業者証明書（$MCert_A$）等、いくつかのデータ要素を含んでいる。なお、内部機密ＫＰＶＡは、デバイスＡのセキュア・セクション内で作成されており、セキュア・セクション外部、及び製造業者に対してさえも開示される必要は無い。デバイスＡは、２つのメッセージＭ１及びＭ２を作成し、それらメッセージをデバイスＢに送信する。メッセージＭ１は、ＫＰＶＡによって署名されたID_A及びＫＰＢＡ１を含んでいる。

【００４０】デバイスＢは、Ｍ１及びＭ２を受信すると、ＫＰＢＳＩＧＭ、すなわち製造業者公開署名キーを用いて、Ｍ２の検査すなわち認証を行う（ステップＳ２）。Ｍ２が有効でない場合、デバイスＢはプロセスを停止して、デバイスＡが権限の無いデバイスすなわち非認可デバイスであると推定する。有効である場合、デバイスＢは、Ｍ２からＫＰＢＡを抽出する（ステップＳ３）。ＫＰＢＡはキーの公開部分であり、ＫＰＶＡはキーの秘密部分である。先に説明したように、公開部分は、製造業者証明書に含まれていたものである。この時点で、デバイスＢは、製造業者が証明したことにより、ＫＰＢＡが実際にはキーの公開部分であると確認する。

【００４１】ステップＳ４において、デバイスＢは、ＫＰＢＡを用いてＭ１を照合する。Ｍ１が有効でない場合、デバイスＢはプロセスを停止し、デバイスＡが非認可デバイスであると推定する。Ｍ１が有効である場合、デバイスＢは、Ｍ１からＫＰＢＡ１を抽出する（ステップＳ５）。この時点で、デバイスＢは、デバイスＡを認証したことになる。デバイスＢを認証するデバイスＡのプロセスには、ステップＳ６～Ｓ１１が含まれる。なお、ステップＳ１～Ｓ５は、ステップＳ６～Ｓ１１に対して特定の順序で発生する必要はない。しかしながら、Ｍ３及びＭ４をデバイスＢからデバイスＡに渡される機密とすることが望ましい場合、デバイスＢは、少なくともデバイスＢにおいて共有機密を生成するために十分なステップを実行することができる。

【００４２】ステップＳ６において、デバイスＢは、認証のために自身のキー・ペア（ＫＰＶＢ１，ＫＰＢＢ１）を生成する。デバイスＡと同様に、正式に製造され

たデバイスＢは、いくつかのデータ要素を有している。デバイスＢにおけるそれらデータ要素には、一意的な識別子（図５のID_B）、内部機密ＫＰＶＢ及びデバイスＢの製造業者証明書（$MCert_B$）が含まれる。内部機密ＫＰＶＢは、デバイスＢのセキュア・セクション内で作成されており、セキュア・セクション外部に開示される必要はない。ＫＰＶＢ１は、後のステップにおいて、共有機密を生成するために用いられる。デバイスＢは、２つのメッセージ、すなわちＭ３、Ｍ４を作成し、それらメッセージをデバイスＡに送信する（ステップＳ７）。メッセージＭ３は、ＫＰＶＢによって署名されたID_B及びＫＰＢＢ１を含んでいる。デバイスＡは、Ｍ３及びＭ４を受信すると、ＫＰＢＳＩＧＭ、すなわち製造業者公開署名キーを用い、てＭ４を照合する（ステップＳ８）。Ｍ４が有効でない場合、デバイスＡはプロセスを停止し、デバイスＢが権限の無いデバイスすなわち非認可デバイスであると推定する。有効である場合、デバイスＡは、Ｍ４からＫＰＢＢを抽出する。ＫＰＢＢは、キーの公開部分であり、ＫＰＶＢはキーの秘密部分であって、$MCert_B$に含まれている。この時点で、デバイスＡは、製造業者が証明したことにより、ＫＰＢＢが実際にはキーの公開部分であると確認する。

【００４３】ステップＳ１０において、デバイスＡはＫＰＢＢを用いてＭ３を照合する。Ｍ３が有効でない場合、デバイスＡはプロセスを停止して、デバイスＢが権限の無いデバイスすなわち非認可デバイスであると推定する。Ｍ３が有効である場合、デバイスＡは、Ｍ３からＫＰＢＢ１を抽出する（ステップ１１）。この時点で、デバイスＡは、デバイスＢを認証（承認）しており、デバイスＢはデバイスＡを認証している。更に、この時点で、デバイスＡは、ＫＰＶＡ１及びＫＰＢＢ１を有しており、デバイスＢは、ＫＰＶＢ１及びＫＰＢＡ１を有している。これらの２つの値の各々を用いて、各デバイスは、共有機密を生成することができる。各デバイスが共有機密を生成すると、２つのデバイスは、共有機密（Ｓ１２Ａ，Ｓ１２Ｂ）を使用することによって、互いの間で機密に通信することができる。共有機密を生成するための方法を後述するが、他の方法を用いて共有機密を生成することも可能である。システムによっては、ＫＰＢＳＩＧＭのセキュリティによらずに共有機密を生成することが好ましい場合もあり、それによってオペレータのシステムはＫＰＢＳＩＧＭが危険に晒された後に危険に晒されることはない。

【００４４】共有機密を生成する１つの方法は、Ｄｉｆｆｅ－Ｈｅｌｌｍａｎ（ＤＨ）交換である。ＤＨ交換は、機密であっても無くてもよい２つの変数、α及びｎを使用するものであり、ただし$\alpha<n$である。デバイスＡは、$KPBA1=\alpha^{KPVA1} mod (n)$であるキー・ペアを生成し、デバイスＢは、$KPBB1=\alpha^{KPVB1} mod (n)$であるキー・ペアを生成する。デバイスＡは、Ｍ３からＫＰＢＢ１を抽出すると、$Y_A=KPBB1^{KPVA1} mod (n)$を計算することができ、デバイスＢは、Ｍ１からＫＰＢＡ１を抽出すると、$Y_B=KPBA1^{KPVB1} mod (n)$を計算することができる。なお、これら値が生成された方法から、以下のように表すことができる。

$Y_A=KPBB1^{KPVA1} mod (n)$
$=(\alpha^{KPVB1})^{KPVA1} mod (n)$
$=(\alpha^{KPVA1})^{KPVB1} mod (n)$
$=KPBA1^{KPVB1} mod (n)$
$=Y_B$

従って、$Y_A=Y_B$であって個別のアルゴリズムを実行することが困難であるため、デバイスＡ及びＢは共有機密を有する。ある実施の形態において、ｎは大きい素数（１０２４ビットのオーダ）であり、αは2^qの元を有する有限体の１つの元である（ｑは、ｎ－１及びαを除算する１６０ビットの素数）。$Y=Y_A=Y_B$が１０２４ビットのオーダである場合、５６ビットＤＥＳキー等のキーをＹから作成することができる。共有機密が作成されると、該共通機密を種々の使用法で用いることができる。

【００４５】図３は、記憶装置３４に記憶されたデータ値の詳細を示している。より詳細には、記憶装置３４は、以下に示す要素に対する記憶領域を含む。

バージョン番号　端末がセキュア・チャネル及び／又は交換キーをセットアップするために使用するプロトコルのバージョン
ＳＳＩＤ　特定の端末／ターゲットＳＳに一意の、製造業者が割当てた値
許可フラグ　いかなる作用が可能であるかを示すフラグ
キーロードタイプ　初期自動キー・ロード・プロセスにおいて発生するキー・ロードのタイプ（例：キー交換キー、一時スーパ・キー、端末キー・ロード・キー
ＫＳＳ　端末用のキー・ペア（ＫＰＶＳＳ，ＫＰＢＳＳ）
ＫＰＢＳＩＧＭ　製造業者の署名キーの公開部分
ＭＣｅｒｔ　製造業者証明書：ターゲットＳＳのオペレータに特有の製造業者キーを用いたＫＳＳの署名（署名されたデータには、バージョン番号、ＳＳＩＤ、許可フラグ及びＫＳＳが含まれる）
ＣＤ　チェック数字

【００４６】ＭＣｅｒｔに許可フラグが含まれている場合、端末は、一旦ＭＩＦによって割当てられるとその許可を変更することができない。許可フラグは、オペレータによって要求されると、端末が実行することができる機能を制限するために、製造業者によってセットされる。例えば、許可フラグは、以下のものを示すことができる。

ａ．ＭＦＫを複数のセキュリティ・モジュール間で共有

することができるか。
ｂ．端末が他のＭＦＫをロードすることが許可されているか。
ｃ．端末にアプリケーション・プログラムをローディングする。
ｄ．端末がキー交換キー（ＫＥＫ）をローディングすることが許可されているか。
ｅ．端末が特定の端末キーをローディングすることが許可されているか。
ｆ．ＤＳＡ署名が照合されるべきか。
【００４７】端末１４の特定の目的は、この開示の主要な面ではないが、端末１４は、購入者情報を収集するか又は電子取引をもたらすために使用されるポイント・オブ・セール（ＰＯＳ）端末か、自動預金支払機（「ＡＴＭ」）か、スマート・カード・リーダ等であってもよい。場合によっては、端末１４は、ある特定の目的に対するセキュリティ・モジュール２４、及び端末製造業者又は後に付加された別個のセキュリティ・モジュールの製造業者によって製造されたセキュリティ・モジュール無しに、製造されてもよい。例えば、ＡＴＭを、セキュリティ・モジュール無しに、ＡＴＭに特有のロジックで製造することができる。そして、ＡＴＭに特有でないセキュリティ・モジュールをＡＴＭに付加することが可能である。
【００４８】他の例では、端末はパーソナル・コンピュータであり、セキュリティ・モジュールはそのパーソナル・コンピュータにインストールされたＰＣＩバス・カードである。パーソナル・コンピュータとセキュリティ・モジュールとが１つの会社によって製造されている場合、パーソナル・コンピュータは、プレインストールされたセキュリティ・モジュールを備えて出荷することができる。初期化が製造時に行われることにより、パーソナル・コンピュータは、オペレータに関連して特有に製造される必要はなく、それにより、オペレータにパーソナル・コンピュータを提供するプロセスが簡略化される。
【００４９】大規模機構組織は、何万台ものパーソナル・コンピュータを使用する可能性があり、それらにはすべて、パーソナル・コンピュータが安全でないネットワーク上で安全に相互通信することができるように、セキュリティ・モジュールがインストールされている必要がある。上述したようなセキュリティ・モジュールが無い場合、組織は、マスタ・ファイル・キー等の、機構組織の機密を含む、特に組織に対して特別に事前に環境設定されたセキュリティ・モジュールを有する必要があるか、あるいは、パーソナル・コンピュータのインストールの時点まで、それら組織の機密を安全に移送するためのインフラストラクチャを必要とする。しかしながら、上述したセキュリティモジュールを有することにより、機構組織は、中央で、それ自身のキーを管理し、好ましくは組織内のパーソナル・コンピュータのエンド・ユーザに透過的な方法で、それらを信頼性の無いチャネル上で分配させることができる。エンド・ユーザは、初期化ルーチンを実行する必要があるだけであり、その後、セキュリティ・モジュールを起動して、図５に示す相互認証プロセスを実行し、キー・サーバから動作のためのキーを取得することができる。
【００５０】図６は、デバイスをオペレータ特有にするために汎用デバイスにキーをローディングするための、信頼性の無いネットワークに接続される可能性のあるキー・サーバ１５０を示している。１つの実現例において、キー・サーバ１５０は、安全な物理的環境にあるウインドウズ（登録商標）ＮＴサーバである。キー・サーバ１５０は、サーバ・ソフトウェア１５２、端末データベース１５４、監査ログ１５６、及びネットワークＩ／Ｏ１５８を備えている。ネットワークＩ／Ｏ１５８は、キー・サーバ１５０を信頼性の無いネットワーク１２に接続すると共に、保護されたコネクションを介して、キー・サーバ１５０をセキュリティ制御端末（ＳＣＴ）１６０に接続する。図示されているように、ＳＣＴ１６０は、保護されたすなわち安全なＩ／Ｏ１６２を介して、ユーザに対するインタフェースを有している。
【００５１】端末データベース１５４は、セキュア・セクションの各々のＭＣｅｒｔと同様に、オペレータが使用する各セキュア・セクションに対する通し番号（ＳＳＩＤ）のリストを保持している。オペレータは、更に多くの端末をオンライン化する時、新たな端末各々に対し、端末データベース１５４にＳＳＩＤ及びＭＣｅｒｔを付加することができる。
【００５２】キー・サーバ１５０内における暗号化動作は、キー・サーバ１５０内のセキュリティ・モジュール２４’によって実行される。キー・サーバ１５０が複数のサブネットワークを管理している場合、キー・サーバ１５０内で、複数のセキュリティ・モジュール２４’が使用されてもよい。セキュリティ・モジュール２４’を上述したセキュリティ・モジュール２４を同じのものとすることができるが、キー・サーバによっては、自動キー生成機能が必要とされないものもある。その代りに、キー・サーバの初期キーが安全なコネクションに亙ってマニュアルでロードされる。安全なコネクションの１つは、ＳＣＴ１６０によって提供され、安全な方法でマスタ・ファイル・キー（ＭＦＫ）をローディングし、セキュア・セクションからデータを読出すことができるものである。
【００５３】上述した方法で、データ完全性もデータ機密性も保証されていない安全でない非セキュア・チャネルを介して、１つ端末と１つのキー・サーバ、又は２つの端末同士を安全に接続させることができ、安全にメッセージを通信し、他のパーティの会話に対する権限を照合することができる。これにより、２つの端末はそれら

の間でメッセージを通信するか、共有機密をセットアップするか、又は非セキュア・チャネルによりキーの安全なローディングを調整することが可能になる。例えば、図５に示すプロセスが完了すると、キー・サーバは、キー又は「キー変更」コマンドの新たなセットをＳＳに安全に送信することができ、ＳＳは、キー・サーバがキーの変更の前に要求されたものであることを照合することができる。

【００５４】誰かが検出されずに許可されていないデバイスをネットワークに挿入し、それをキー・サーバによって照合させることを防止するために、キー・サーバはキー・サーバがそれを用いて実行した端末の監査ログ１５６を保持する。監査ログ１５６の記録には、端末の製造業者製造ＩＤ（ＳＳＩＤ）と、通し記録番号とが含まれる。通し記録番号は、監査ログ１５６からの記録の削除を明らかにする。変更を防止するために、記録は署名されていることが可能である。ここでは、キーの初期セットをロードするために安全なチャネルを必要とすることなく、１つ又は複数のキーの初期セットをロードするシステムが説明された。このシステムにより、安全でないネットワークを介してセキュア・セクションを安全に初期化し認証することができる。

【００５５】上述した説明は、例示的なものであって限定的なものではない。当業者には、この開示を検討することにより本発明の多くの変形例が明らかとなろう。従って、本発明の範囲は上記説明に関して判断されるべきではなく、添付の特許請求の範囲とそれらの同等物の全範囲とに関して判断されるべきである。

【図面の簡単な説明】

【図１】ネットワークに相互接続された保護されたデバイスのブロック図である。

【図２】セキュア・セクションを有するセキュリティ・モジュールを含む、図１の保護されたデバイスの詳細なブロック図である。

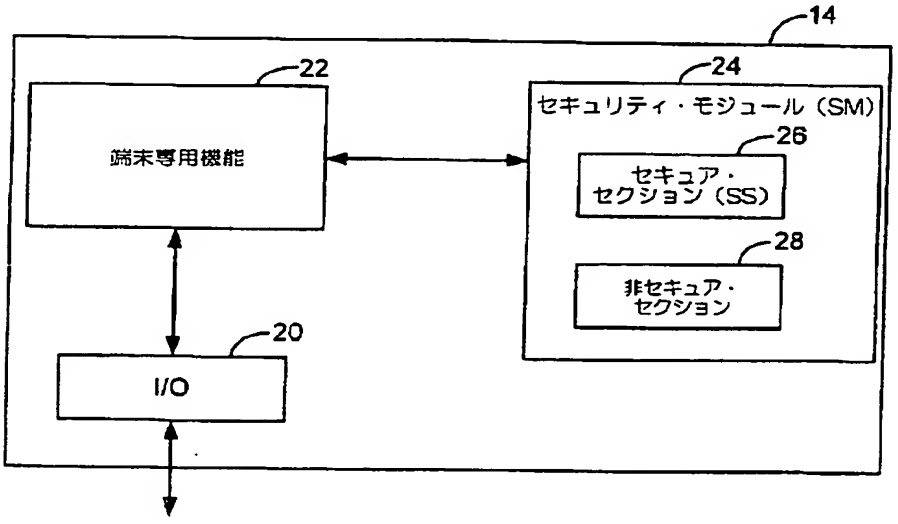
【図３】図２のセキュア・セクションの詳細なブロック図である。

【図４】図１～図３に示されているデバイスに対する製造初期化プロセスを示す製造初期化ファシリティのブロック図である。

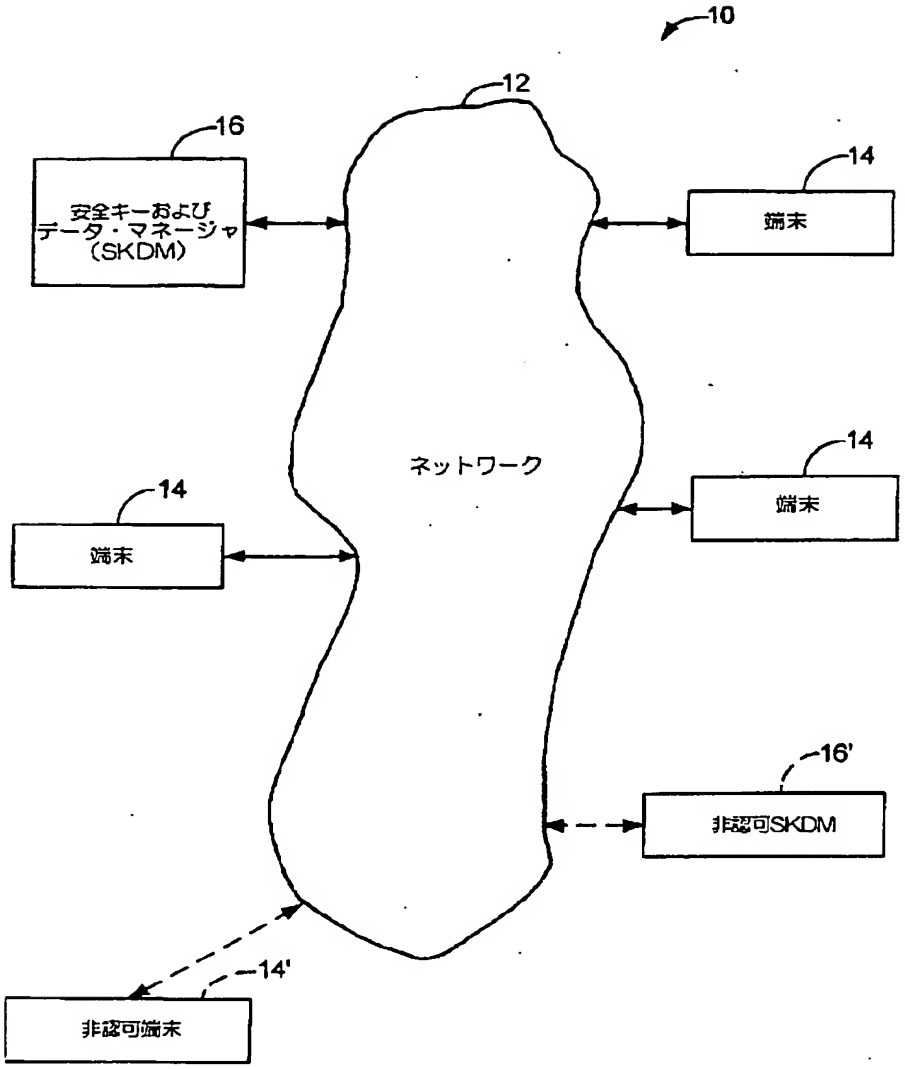
【図５】信頼性の無いチャネルによって接続された２つのデバイス間に発生する自動キー初期化、相互認証、及び共有機密生成のプロセスのフローチャートである。

【図６】自動キープロセスを用いてネットワークに結合されたデバイスを初期化するために、図１に示すネットワークによって使用されるキー・サーバのブロック図である。

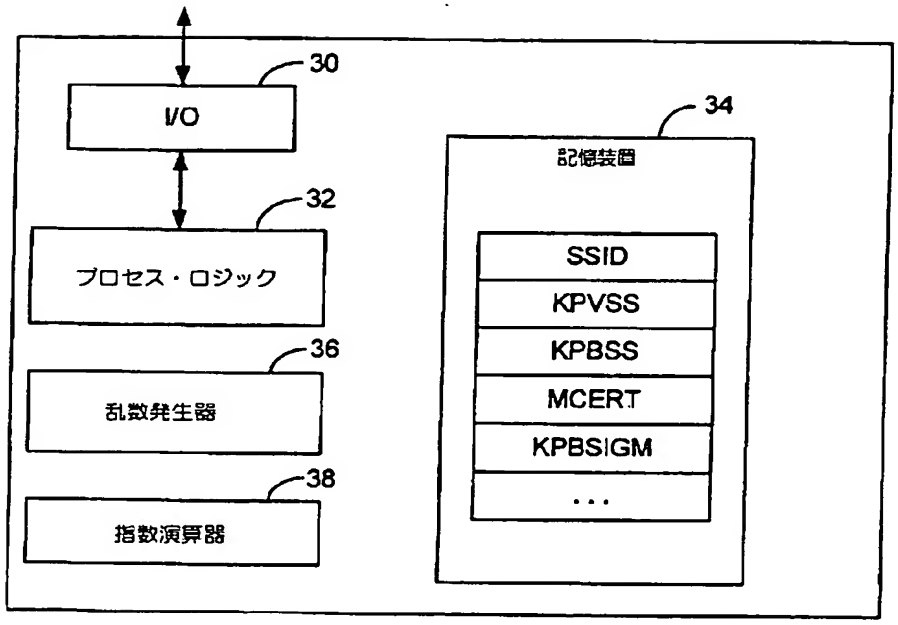
【図２】



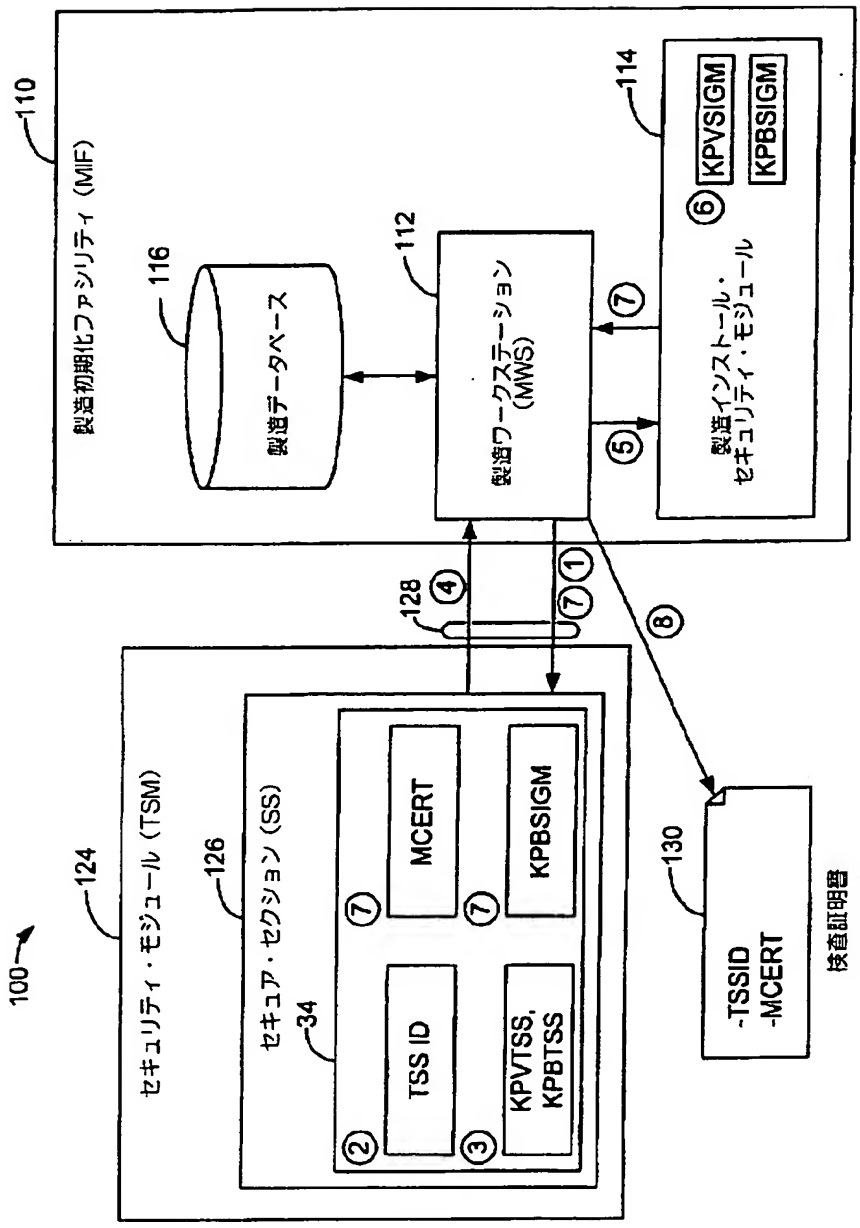
【図１】


10
12
16
安全キーおよび
データ・マネージャ
(SKDM)
14
端末
ネットワーク
14
端末
14
端末
16'
非認可SKDM
14'
非認可端末

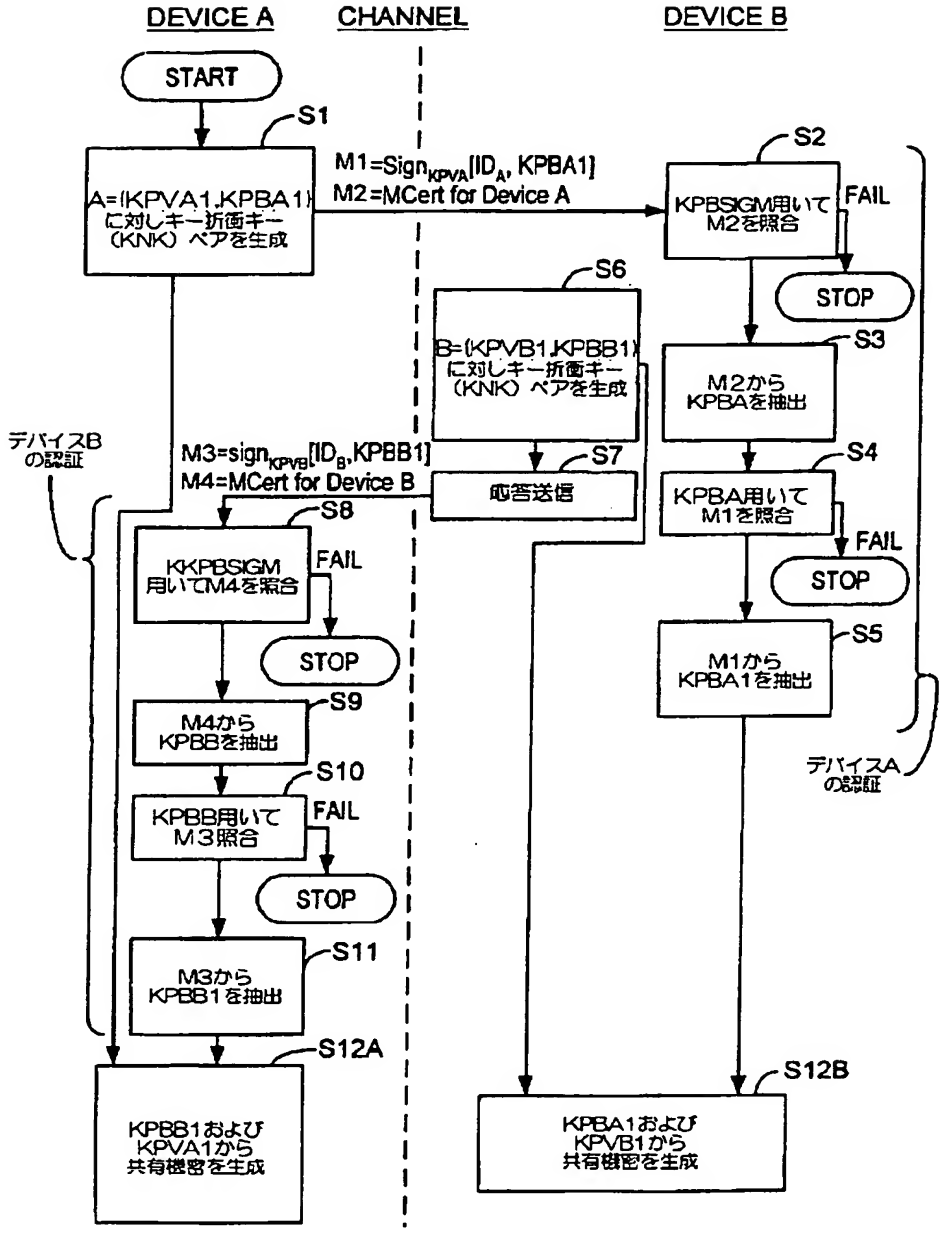
【図３】


30
I/O
32
プロセス・ロジック
36
乱数発生器
38
指数演算器
34
記憶装置
SSID
KPVSS
KPBSS
MCERT
KPBSIGM
...

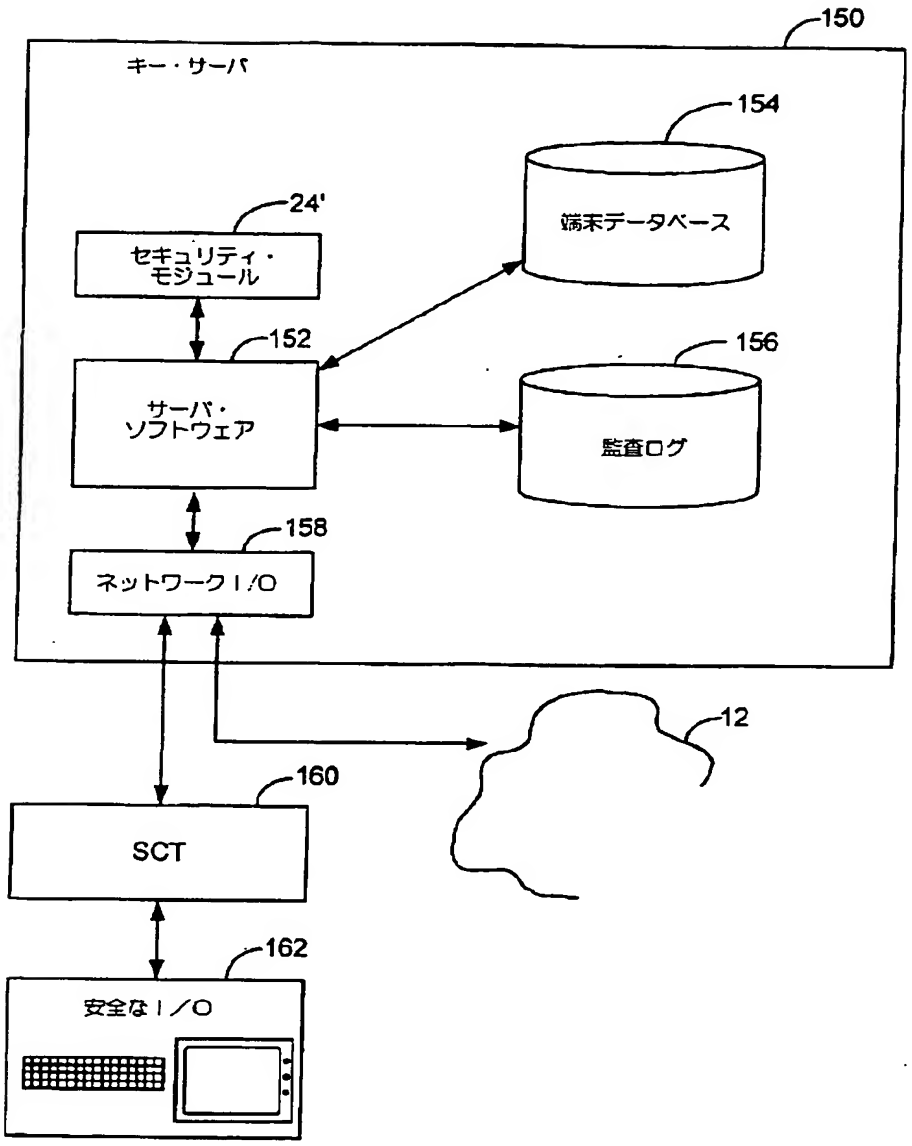
【図4】


製造初期化ファシリティ（MIF）
110
製造データベース
116
製造ワークステーション（MWS）
112
製造インストール・セキュリティ・モジュール
114
KPVSIGM
KPBSIGM
⑥
⑤
⑦
①
④
128
⑧
セキュリティ・モジュール（TSM）
124
セキュア・セクション（SS）
126
34
TSS ID
KPVTSS, KPBTSS
MCERT
KPBSIGM
②
③
⑦
⑦
100
130
-TSSID
-MCERT
検査証明書

【図５】


DEVICE A
CHANNEL
DEVICE B
START
S1
A=(KPVA1,KPBA1)
に対しキー折衝キー
(KNK) ペアを生成
M1=Sign$_{KPVA}$[ID$_A$, KPBA1]
M2=MCert for Device A
S2
KPBSIGM用いて
M2を照合
FAIL
STOP
S6
B=(KPVB1,KPBB1)
に対しキー折衝キー
(KNK) ペアを生成
S3
M2から
KPBAを抽出
S4
KPBA用いて
M1を照合
FAIL
STOP
S5
M1から
KPBA1を抽出
デバイスA
の認証
デバイスB
の認証
M3=sign$_{KPVB}$[ID$_B$,KPBB1]
M4=MCert for Device B
S7
応答送信
S8
KKPBSIGM
用いてM4を照合
FAIL
STOP
S9
M4から
KPBBを抽出
S10
KPBB用いて
M3照合
FAIL
STOP
S11
M3から
KPBB1を抽出
S12A
KPBB1および
KPVA1から
共有機密を生成
S12B
KPBA1および
KPVB1から
共有機密を生成

【図６】



フロントページの続き

(71)出願人 591030868
20555 State Highway 249, Houston, Texas 77070, United States of America
(72)発明者 マイケル・マッケイ
アメリカ合衆国カリフォルニア州，ベンロモンド，グレンアーバー・ロード 8727
(72)発明者 スーザン・ラングフォード
アメリカ合衆国カリフォルニア州，サニーヴェイル，ポプラ・アベニュー 1275，ナンバー 101
(72)発明者 ラリー・ハイネス
アメリカ合衆国カリフォルニア州，サンタ・クララ，パークビュー・ドライブ 610，ナンバー 105